AO 106 (Rev. 01/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of California

FILED
09 AUG 11 AM 9:48

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
GOOGLE INC.
1600 AMPHITHEATRE WAY
MOUNTAIN VIEW, CALIFORNIA

SEALED Unsealed on 3/16/10

Case No.
'09 MJ2406

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Northern District of California *(identify the person or describe property to be searched and give its location):* Google Inc., 1600 Amphitheatre Way, Mountain View, California (as further described in Attachment A)

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*: See Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 371, 554, and the application is based on these facts: And also 50 U.S.C. Section 1705.
See Attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Matthew R. Murphy, Special Agent, ICE
Printed name and title

Sworn to before me and signed in my presence.

Date: 8/11/09

Judge's signature

City and state: San Diego, California

Jan M. Adler, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF

APPLICATION FOR SEARCH WARRANT

I, Matthew R. Murphy, being duly sworn, hereby depose and state as follows:

1. I am a Special Agent (SA) of U.S. Immigration and Customs Enforcement (ICE), and have been so employed since June 2003. I am a graduate of the Federal Law Enforcement Training Center (FLETC), Glynco, Georgia. At FLETC, I was trained in, among other things, criminal investigative techniques. I have participated in criminal investigations involving, among other things, the illegal export of military and defense articles and "dual use" items (used in both civil and military functions) out of the United States. I have received formal training in the laws and regulations relating to the International Emergency Economic Powers Act (IEEPA), 50 U.S.C 1705, and Smuggling Goods from the United States, in violation of 18 U.S.C. 554. I have conducted and participated in investigations of the above listed laws and regulations.

2. This affidavit is in support of an application for a search warrant for Google Inc. ("Google"). I seek authority to search Google, 1600 Amphitheatre Way, Mountain View, California, as described in Attachment A, for records associated with the Google e-mail or user account essi.taghavi@gmail.com as described in Attachment A, Section II (the "Subject E-mail Account"). As set forth below, there is probable cause to believe that located within the Subject E-mail Account is evidence ESMAEIL TAGHAVI has conspired, and is conspiring, to export U.S. goods and technology from the Untied States to Iran, in violation of the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. § 1705, and in violation of 18 U.S.C. § 554 (Smuggling Goods from the United States), all in violation of 18 U.S.C. § 371.

3. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation (including law enforcement officers), my review of documents and computer records related to this investigation, and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, it does not set forth every fact that I or others have learned during the investigation.

STATEMENT OF PROBABLE CAUSE

A. Legal Background

IEEPA and the Iranian Transaction Regulations

4. Pursuant to the authority under the International Emergency Economic Powers Act (IEEPA), the President of the United States and the executive branch have issued orders and regulations governing and prohibiting certain transactions with the Islamic Republic of Iran (Iran) by U.S. persons or involving U.S. goods. Title 50, United States Code, Section 1705 provides:

> (a) Unlawful acts. It shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under [the International Emergency Economic Powers Act].
>
> (b) . . .
>
> (c) Criminal penalty. A person who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids and abets in the commission of, an unlawful act described in subsection (a) shall, upon conviction, be fined . . ., or if a natural person, may be imprisoned for not more than 20 years, or both.

5. Pursuant to the Executive Order by President William Jefferson Clinton in 1995, the Secretary of the United States Department of Treasury, in consultation with the Secretary of State, promulgated the Iranian Transaction Regulations, Title 31, United States Code of Federal

Regulations, Part 560. The Iranian Transaction Regulations generally prohibit any person from exporting or causing to be exported from the United States to Iran without a license most goods or technology without having first obtained a validated export license from the United States Department of Treasury, Office of Foreign Assets Control (OFAC).

6. The Iranian Transaction Regulations imposed, among others, the following prohibitions:

> Section 560.204: Prohibited exportation, reexportation, sale or supply of goods, technology, or services to Iran.
>
> Except as otherwise authorized . . . the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, technology, or services to Iran or the Government of Iran is prohibited . . .
>
> Section 560.203: Evasions; attempts.
>
> Any transaction by any United States person or within the United States that evades or avoids, or has the purpose of evading or avoiding, or attempts to violate, any of the prohibitions contained in this part is hereby prohibited.

B. Investigation of Esmaeil Taghavi

7. On April 16, 2009, I received subpoena information from Google Inc. related to the email account essi.taghavi@gmail.com. The subpoena information indicated the account was opened by ESSI TAGHAVI on October 3, 2005.

8. On April 24, 2009, I served an order for a Pen Register and Trap and Trace device on TAGHAVI'S email account essi.taghavi@gmail.com. The following information was derived from the results obtained via the order:

> On April 28, 2009, an individual logged into the email account essi.taghavi@gmail.com using Internet protocol address 77.237.80.114. A search of a commercially available database show the IP address came back to the Internet service provider Saman-Net in Karaj, Iran.

On May 1, 2009, an individual logged into the email account essi.taghavi@gmail.com using Internet protocol address 77.237.80.116. This IP address came back to the Internet service provider Saman-Net in Karaj, Iran.

On May 6, 2009, an individual logged into the email account essi.taghavi@gmail.com using Internet protocol address 77.237.80.34. This IP address came back to the Internet service provider Saman-Net in Karaj, Iran.

On May 10, 2009, an individual logged into the email account essi.taghavi@gmail.com using Internet protocol address 217.219.177.246. This IP address came back to the Internet service provider Pinar Communication in Ginbar, Iran.

On May 28, 2009, an individual logged into the email account essi.taghavi@gmail.com using Internet protocol address 212.33.207.235. This IP address came back to the Internet service provider Fanavaran Ettelaaat Dibaragan Karaj Co. Ltd. in Tehran, Iran.

On May 30, 2009, an individual logged into the email account essi.taghavi@gmail.com using the Internet protocol address 212.33.207.236. This IP address came back to the Internet service provider Fanavaran Ettelaaat Dibaragan Karaj Co. Ltd. in Tehran, Iran.

On June 1, 2009, an individual logged into the email account essi.taghavi@gmail.com using the Internet protocol address 85.133.222.153. This IP address came back to the internet service provider Sepanta Communication Development Co. Ltd., Tehran, Iran.

9. On July 8, 2009, a cooperating source (CS) conducted a consensual monitored meeting with ESMAEIL TAGHAVI for approximately two hours at TAGHAVI'S business, San Diego EZ Riders, located at 851 West Mission Avenue, Unit B, Escondido, CA 92025. The conversation took place in the Farsi language. The conversation was translated by Language Specialist Mamad Shirazi, Department of Homeland Security's Interpreter's Unit. My review of the translation transcripts revealed that TAGHAVI informed the CS he was attempting to set up a business transaction to send thousands of laptop computers to Iran. In addition, TAGHAVI explained how the laptops would be trans-shipped through London. During the meeting, TAGHAVI asked the CS to set up a meeting with an individual who might be able to assist with the business transaction.

10. On July 8, 2009, while discussing the transaction to supply Iran with laptops, TAGHAVAI made reference to a "Mr. Azadbakht" as the individual who would provide the purchase price:

> "Look, the good thing about it is that Mr. Azad-" what was it? Azadbakht? Nikbakht? - he said, "He does all the..." Of course, he himself had said the same thing to me, he said, "Regarding how much you sell it for, you don't have a problem, because we tell you what our purchase price is."

Later in the conversation, TAGHAVI referred to Azadbakht again:

TAGHAVI: And I am telling you, in Iran, they are still educating on computers. Here, laptops are dying out.

CS: Out, yeah.

TAGHAVI: I told you 2011...I was talking to Haji that day, I said these...until when do these m_____f_____rs want to ...He said, "In Iran, you know

[Loud microphone noise]

if we can work with the system for three years, that is enough." That means, after three years, automatically they put us away-

CS: Yeah, they put aside, yeah.

TAGHAVI: Why? Because there are groups.

CS: Yeah, there are factions.

TAGHAVI: The president changes, all the heads and groups change.

CS: Yeah.

TAGHAVI: At the time of Mohsen Rafighdoust, do you know what these guys Hamid (UI) and Javad took with them? They left, another group, they left, another group. Ah, let me tell you something interesting. All of these, and do you know what they told me at the end, why they asked me to wait another 10 days? They wanted to do whatever they were going to do after the election. Because they had a one percent doubt that-

CS: Ahmadinejad may not win.

TAGHAVI: Ahmadinejad, how do you say, their group would fall apart. That's why they kept telling me, "Wait another ten days."
In the same meeting, I turned around and said, "I won't wait ten days, I won't wait one day either. But I am sure I will come back." He said why? I mean, I knew that Ahmadinejad is what-do-you-call-it…I knew, I said, "Nothing is gonna change, I'll be back."
Haji said, he said, "Yesterday Mr. Azadbakht had said that Mr. Taghavi likes Mr. Ahmadinejad very much and he very much knew when he said that."
If I knew, this was something-

CS: It was obvious.

TAGHAVI: this was written all over. There are so much forgeries in that country-

11. Results from the pen register order on TAGHAVI'S email account essi.taghavi@gmail.com, show TAGHAVI utilized that account to send the following four emails:

On August 3, 2009, TAGHAVI sent an email to the account h.azadbakht51@gmail.com;

On July 29, 2009, TAGHAVI sent an email to the account h.azadbakht51@gmail.com;

On July 11, 2009, TAGHAVI sent an email to the account h_azad@mail.com;

On June 1, 2009, TAGHAVI sent an email to the account h_azad@mail.com.

12. On July 31, 2009, an undercover agent (UCA) with the Defense Criminal Investigative Service (DCIS) and the CS had a consensual monitored meeting with TAGHAVI at Starbucks, 1435 Camino Del Mar, Del Mar, California. My review of the consensually monitored conversation revealed the following in substance. During the meeting, TAGHAVI informed the UCA he had a big customer in an Arabic country that he was in the process of doing a nine million dollar deal with for approximately 20,000 "toughbook" computers. TAGHAVI explained he was not an employee of the Iranian Government, but that he had friends high up in the government there and wanted to use those connections to make millions of dollars.

The UCA stressed the importance of being discreet when shipping the computers overseas, at which time TAGHAVI stated, "I want to cover my ass too, dude." TAGHAVI stated he knew there were embargoes and sanctions against Iran. When discussing payment and financing terms, TAGHAVI stated he was concerned with receiving several million dollars in one of his bank accounts and having the Government ask him where it came from. TAGHAVI informed the UCA they would not need to worry about the deal because they would just be shipping the laptops to London, and the line of credit would be opened for them from London. The meeting closed with TAGHAVI stating, "These computer buyers, I think they are from Iran, but I don't know, as you said, we don't want to know." TAGHAVI went on to explain the customer would open a letter of credit from London and then TAGHAVI and the UCA would ship the laptops to London or Dubai." During the meeting, TAGHAVI and the UCA also discussed the possibility that the UCA could provide TAGHAVI with military goods in the future that would be shipped to a customer TAGAVHI had in Iran. TAGHAVI provided the UCA with his email account essi.taghavi@gmail.com and telephone number for the purposes of future communication. When discussing communication, TAGHAVI stated he knew the UCA knew what he/she was doing, but that it was important to be cautious in the email.

13. On July 31, 2009, the UCA emailed TAGHAVI at the email account essi.taghavi@gmail.com. In the email, the UCA provided TAGHAVI with a contact phone number and email address and stated he/she would look into supplying 5,000 laptops per month like TAGHAVI wanted.

14. On August 2, 2009, TAGHAVI emailed the UCA utilizing the email account essi.taghavi@gmail.com. In the email, TAGHAVI stated he had just had a phone conversation

and the customers are looking for the latest model HP and Sony laptops in large quantities. TAGHAVI asked the UCA to make some offers to them.

15. On August 3, 2009, the UCA emailed TAGHAVI at the email account essi.taghavi@gmail.com. In the email the UCA stated he/she had a call into Sony for competitive pricing in large quantities and had contacted some other people regarding sourcing the laptops outside of the manufacturers. The UCA stated he/she would be in touch as soon as he had some answers.

16. On August 6, 2009, the UCA emailed TAGHAVI at the email account essi.taghavi@gmail.com. In the email the UCA stated he/she had come up with a way to purchase directly from Hewlett Packard (HP). The UCA asked TAGHAVI for additional details on the specific type of laptop the customer wanted. The UCA informed TAGHAVI he/she could provide between 1600-3200 laptops per month and asked how TAGHAVI preferred to handle financing.

17. In sum, during the consensually monitored meetings with the CS and UCA, TAGHAVI explained he was attempting to finalize transactions to supply laptop computers to Iran in violation of the current embargo. TAGHAVI has been utilizing his email account essi.taghavi@gmail.com to communicate with the UCA in furtherance of sending the laptops to Iran. TAGHAVI utilized the account essi.taghavi@gmail.com to email Azadbakht on four occasions in the last few months. An individual (presumably TAGHAVI) accessed the email account essi.taghavi@gmail.com on a regular basis from about April 28, 2009 to June 1, 2009, from Iran. Based on the foregoing, I submit there is probable cause to believe that ESMAEIL TAGHAVI is involved in an ongoing conspiracy to ship laptop computers to Iran in violation of

the current embargo, and that evidence of these violations will be found in the subject email account.

SEARCH PROTOCOL

18. As a federal agent, I am trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of Google are likely not. The manner in which the data is preserved and analyzed may be critical to the successful prosecution of any case based upon this evidence. Computer Forensic Examiners are trained to handle digital evidence. It would be inappropriate and impractical, however, for federal agents to search the vast computer network of Google for the relevant accounts and then to analyze the contents of those accounts on the premises of Google. The impact on Google's business would be severe.

19. Therefore, I request authority to seize all images, text messages and other content from the Google accounts, as described in Attachment A. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Google, authority is sought to allow Google to make a digital copy of the entire contents of the accounts subject to seizure. That copy will be provided to me or to any authorized federal agent. The contents will then be analyzed to identify communications and other data subject to seizure pursuant to Attachment A. Relevant data will be copied to separate media. The original media will be sealed and maintained to establish authenticity, if necessary.

20. Analyzing the data to be provided by Google requires special technical skills, equipment and software. It also can be very tedious. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Certain file formats do not lend themselves to keyword

searches. Keywords search text. Many common electronic mail, database and spreadsheet applications, which files may have been to electronic mail, do not store data as searchable text. The data is saved in a proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases dramatically.

21. Based on the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained; criminals can use code to avoid keyword searches and mislabel files, encrypt files, deliberately misspell certain words and take other steps to defeat law enforcement.

22. All forensic analysis of the recovered data will be directed exclusively to the identification and seizure of information within the scope of this warrant.

REQUEST FOR SEALING AND PRECLUSION OF NOTICE

23. This is an ongoing investigation. It is likely, based upon the above, that evidence of the crimes under investigation exists on computers, and within files, subject to the control of the targets. Based on the foregoing, there is reason to believe that notification of the existence of the search warrant will result in destruction or tampering with evidence and will seriously jeopardize the success of the investigation. Accordingly, it is requested that this warrant and its related materials be sealed until further order of the Court. In addition, pursuant to Title 18, United States Code, Section 2705(b), it is requested that this Court order the electronic service provider to whom this warrant is directed not to notify anyone of the existence of this warrant,

other than its personnel essential to compliance with the execution of this warrant until further order of the Court.

Matthew R. Murphy
Special Agent
U.S. Immigration and Customs Enforcement

Subscribed and sworn to before me this 11th day of August 2009.

HONORABLE JAN M. ADLER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Google Inc. is an Internet service provider located at 1600 Amphitheatre Way, Mountain View, California.

I. Service of Warrant

The officer executing this warrant shall effect service by any lawful method, including faxing the warrant (with Google's consent to fax service) to Google Inc.'s offices described above.

The officer executing the warrant shall permit Google Inc., as custodian of the computer files described in Section II below, to locate the files, copy them onto removable electronic storage media or print them out as paper copies and deliver the same to the officer, who need not be present during this process at the location specified in the warrant.

II. Items subject to seizure

All subscriber and/or user information, all electronic mail, images, text messages, histories, buddy lists, profiles, method of payment, detailed billing records, access logs, transactional data and any other files associated with the following user names and/or email accounts:

essi.taghavi@gmail.com

The search of the data supplied by Google Inc., pursuant to this warrant will be conducted as follows: All images, text messages and other content from the Google Inc. accounts will be seized. To accomplish the objective of the search warrant with a minimum of interference with the business activities of Google Inc., and to effectively pursue the investigation, Google Inc. will make a digital copy of the entire contents of the accounts subject to seizure. That copy will be provided to Special Agent Matthew Murphy, United States Immigration and Customs Enforcement, or to any authorized federal agent. The contents will then be analyzed to identify communications and other data described below. Relevant data will be copied to separate media. The original media will be sealed and maintained to establish authenticity, if necessary.

The search will be limited to securing communications and attachments related to, referring to or evidencing: the purchasing, selling, pricing or quoting of computers or laptop computers; the exportation, reexportation or transhipment of computers or computer components; United States export controls or regulations; Iranian procurement; Azadbakht; and files and records that show dominion and control of the email account listed above, which evidence will tend to prove violations of 18 U.S.C. §§ 371 and 554, and 50 U.S.C. § 1705.